Final Engagement

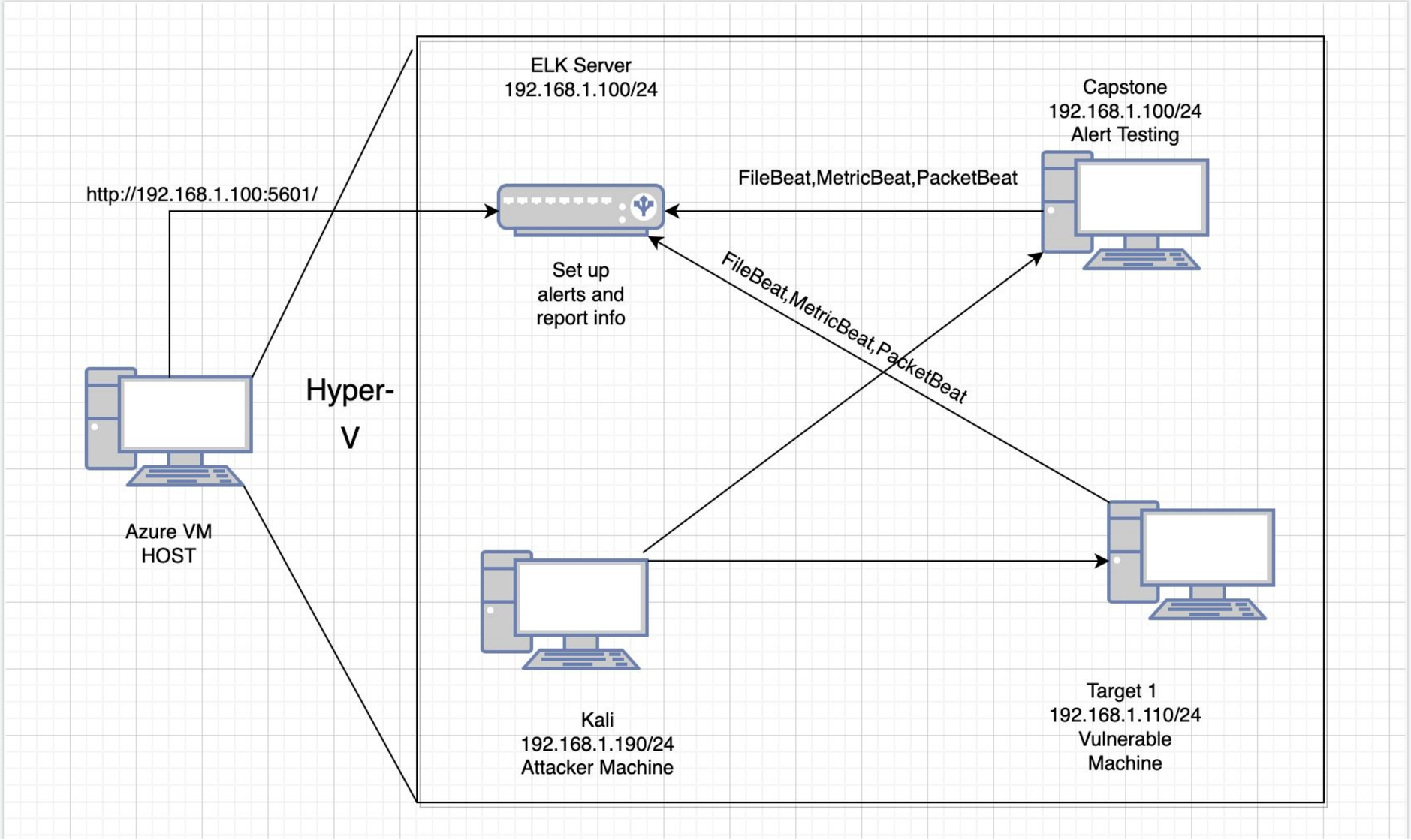
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address
Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS:Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS:Linux
Hostname: Target 1

Critical Vulnerabilities: Target 1

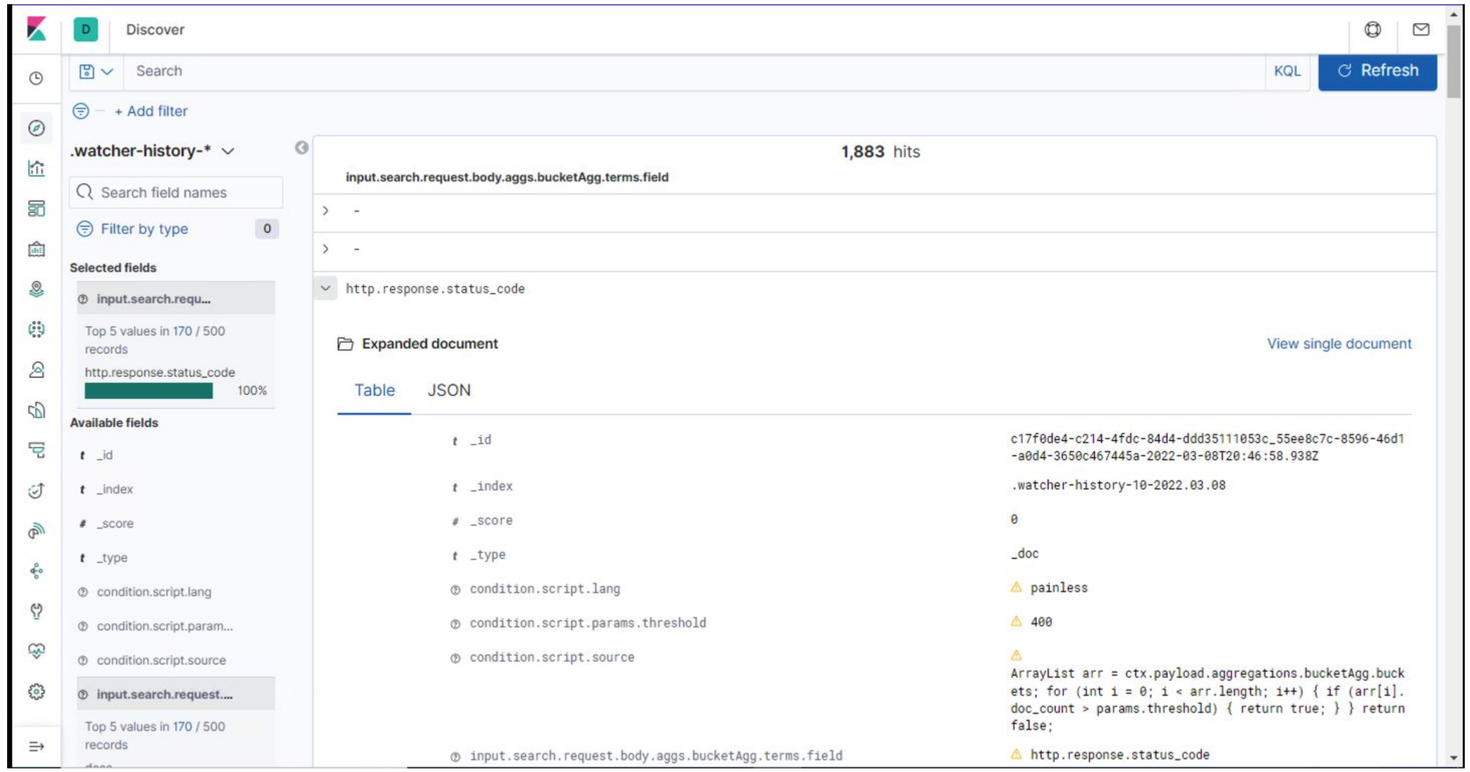
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Weak SSH password	SSH password was easily guessed	Allows access to the users machine
Plaintext DB password	The database password was in plaintext allowing access to Mysql database	This allows the access to the user’s hashes in db
Python misconfiguration	python was configured to allow user to use sudo	The ability to run a python script to allow root access

Alerts Implemented

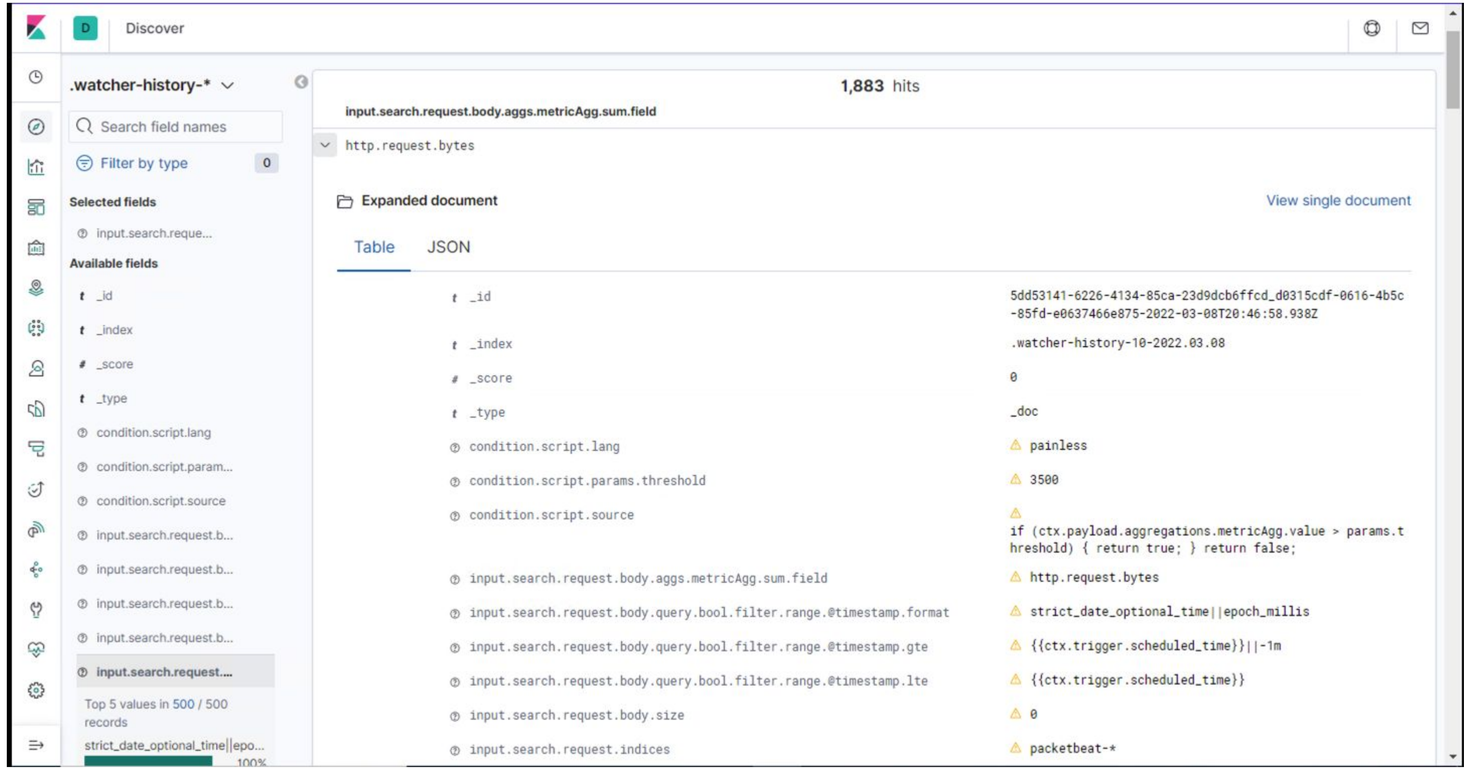
Excessive HTTP Errors

- This monitors for an excessive amount of HTTP errors.
- The alert is set to trigger if the HTTP response status code is above 400 for the last 5 minutes.



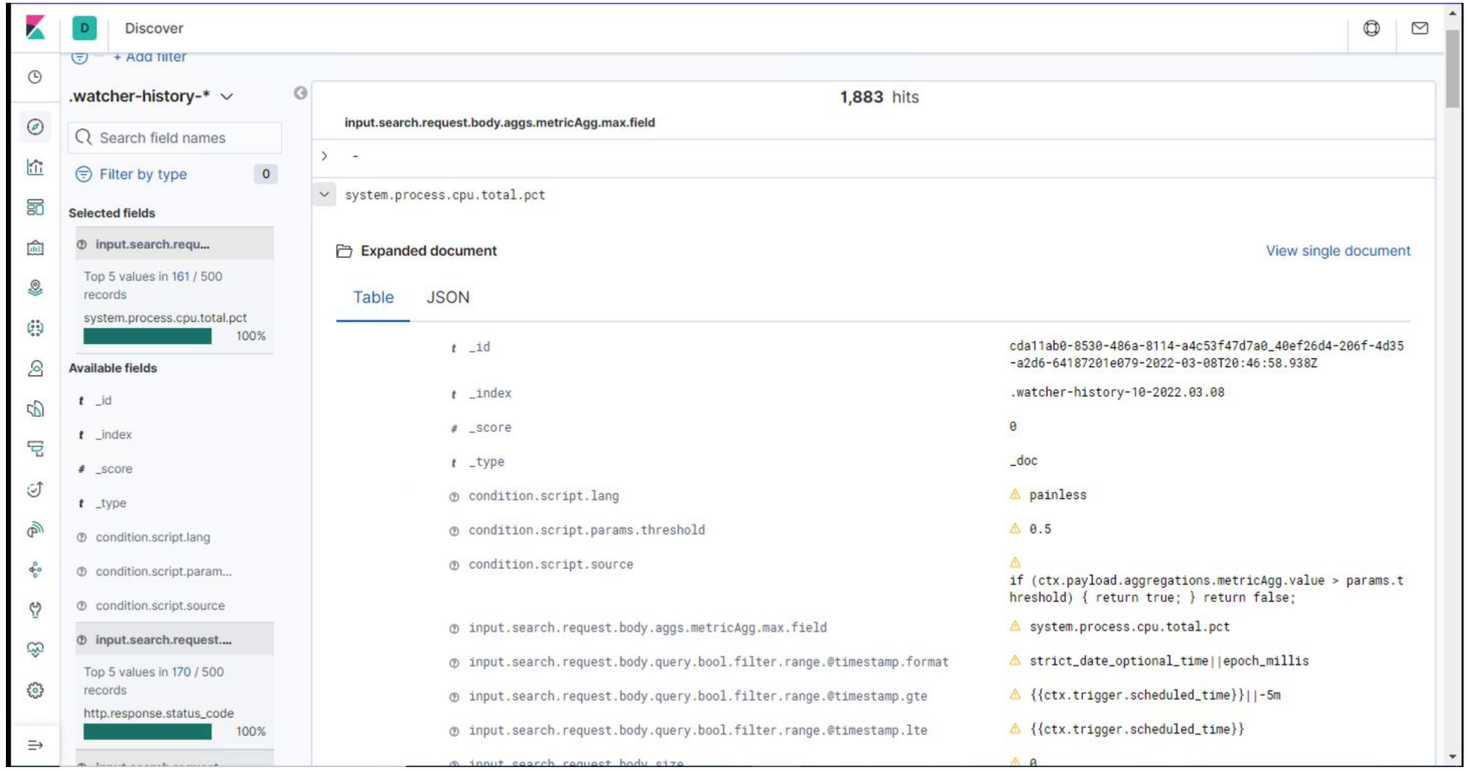
Request HTTP Size Monitor

- This alert monitors the HTTP request bytes across all documents
- The threshold at which the alert is triggered is above 3500 for the last 1 minute



CPU Usage Monitor

- The metric monitored is the total amount of system processes running on the CPU in all documents
- The threshold at which this alert fires is above 0.5 for the last 5 minutes



Hardening

Hardening Against Weak SSH Password on Target 1

Explain how to patch Target 1 against Vulnerability 1.

- Update the SSHD config file
- Navigate to the /etc/ssh/sshd_config file
- vim sshd_config for editing
- Uncomment the passwordauthentication:yes and change it to no.
- This will not allow for users without key verification to log in.

Hardening Against Plaintext DB Password on Target 1

Explain how to patch Target 1 against Vulnerability 2. Include:

- Change the read permissions
- To alter the change of permissions to the file you would execute the command:
- sudo chmod 700 <filename>
- This would allow only the owner of the file to rwx the file. This would prevent anyone other than the owner permissions to the file.The owner can then monitor on an individual basis who should have access.

Hardening Against Python Misconfiguration on Target 1

Explain how to patch Target 1 against Vulnerability 3. Include:

- Edit the visudo file to prevent access to python
- Navigate to the /etc directory
- type sudo visudo
- locate the user with access to python and delete or # the line with that users permissions so that they are no longer allowed access to python.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

Explain which vulnerability each task in the playbook patches.

- The SSH part of the playbook would update the SSH config file and then restart the service.
- The change permissions aspect of the playbook would alter file permissions.
- The playbook for the python aspect would ensure that the user permissions are never altered and automatically configured to the original owners preferences everytime the system starts.